

Lecture Notes in Computer Science  
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

2052

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Singapore*

*Tokyo*

Vladimir I. Gorodetski Victor A. Skormin  
Leonard J. Popyack (Eds.)

# Information Assurance in Computer Networks

Methods, Models and Architectures  
for Network Security

International Workshop MMM-ACNS 2001  
St. Petersburg, Russia, May 21-23, 2001  
Proceedings



Springer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editors

Vladimir I. Gorodetski  
St. Petersburg Institute for Informatics  
and Automation of the Russian Academy of Sciences (SPIIRAS)  
SPIIRAS, 39, 14th Liniya, St. Petersburg, Russia 199178  
E-mail: gor@mail.iias.spb.su

Victor A. Skormin  
Binghamton University, Watson School of Engineering  
Binghamton, NY 13902, USA  
E-mail: vskormin@binghamton.edu

Leonard J. Popyack  
Air Force Research Laboratory  
Defensive Information Warfare Branch  
525 Brooks Road, Rome, NY 13441-4505  
E-mail: Leonard.Popyack@rl.af.mil

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information assurance in computer networks : methods, models, and  
architectures for network security ; proceedings / International  
Workshop MMM ACNS 2001, St. Petersburg, Russia, May 21 - 23, 2001.  
Vladimir I. Gorodetski ... (ed.). - Berlin ; Heidelberg ; New York ;  
Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo :  
Springer, 2001  
(Lecture notes in computer science ; 2052)  
ISBN 3-540-42103-3

CR Subject Classification (1998): C.2, D.4.6, E.3, K.6.5, K.4.1, K.4.4, J.1

ISSN 0302-9743

ISBN 3-540-42103-3 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York  
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2001  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna  
Printed on acid-free paper      SPIN 10781519      06/3142      5 4 3 2 1 0

# Preface

This volume contains the papers selected for presentation at the International Workshop on Mathematical Methods, Models and Architectures for Network Security Systems (MMM-ACNS 2001) held in St. Petersburg, Russia, May 21–23, 2001. The workshop was organized by the St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS) in cooperation with the Russian Foundation for Basic Research (RFBR), the US Air Force Research Laboratory (both the Information Directorate (AFRL/IF)) and the Office of Scientific Research (AFRL/OSR), and Binghamton University (USA).

MMM-ACNS 2001 provided an international forum for sharing original research results and application experiences among specialists in fundamental and applied problems of computer network security. An important distinction of the workshop was its focus on mathematical aspects of information and computer network security and the role of mathematical issues in contemporary and future development of models of secure computing.

A total of 36 papers coming from 12 different countries on significant aspects of both theory and applications of computer network and information security were submitted to MMM-ACNS 2001. Out of them 24 were selected for regular presentation. Five technical sessions were organized, namely: mathematical models for computer networks and applied systems security; methods and models for intrusion detection; mathematical basis and applied techniques of cryptography and steganography; applied techniques of cryptography; and models for access control, authentication, and authorization. Two panel discussions were devoted to the significant issues in the computer and information security field. The first sought to define the important open problems in computer security and to reach a conclusion as to mathematical methods and models can contribute, and the second focused upon security research and education in academia. The MMM-ACNS 2001 program was enriched by five invited speakers: Dipankar Dasgupta, Alexander Grusho, Catherine Meadows, Ravi Sandhu, and Vijay Varadharajan.

An event like this can only succeed as a result of team efforts. We would like to acknowledge the contribution of the Program Committee members and thank the reviewers for their efforts. Our sincere gratitude goes to all of the authors who submitted papers.

We are grateful to our sponsors: the European Office of Aerospace Research and Development (EOARD), the European Office of Naval Research International Field Office (ONRIFO), and the Russian Foundation of Basic Research (RFBR) for their generous support.

We wish to express our thanks to Alfred Hofmann of Springer-Verlag for his help and cooperation.

May 2001

Vladimir Gorodetski  
Leonard Popyack  
Victor Skormin

## MMM-ACNS 2001 Workshop Committee

### General Chairmen:

Victor Skormin	Watson School of Eng., Binghamton Univ., USA
Rafael Yusupov	St. Petersburg Inst. for Informatics and Automation, Russia

### International Organizing Committee

Barry Mckiney	Air Force Research Laboratory/IF, USA
Michael Morgan	Office of Naval Research Int. Field Office, USA
Christopher Reuter	European Office of Aerospace R&D, USA
Rafael Yusupov	St. Petersburg Inst. for Informatics and Automation, Russia

## Program Committee

### Program Co-chairmen:

Vladimir Gorodetski	St. Petersburg Inst. for Informatics and Automation, Russia
Leonard Popyack	Air Force Research Laboratory/IF, USA
Victor Skormin	Watson School of Eng., Binghamton Univ., USA

### International Program Committee

Kurt Bauknecht	Univ. of Zurich, Dept. of Information Technology, Switzerland
Harold Carter	University of Cincinnati, USA
Peter Chen	Computer Science Dept., Louisiana State Univ., USA
Dipankar Dasgupta	Div. of Computer Science, Univ. of Memphis, USA
Jose G. Delgado-Frias	Electrical and Comp. Eng. Dept., Univ. of Virginia, USA
Lynette Drevin	Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Jiri Fridrich	Watson School of Eng., Binghamton Univ., USA
Dimitris Gritzalis	Athens Univ. of Economics & Business, Greece
Alexander Grusho	Russian State Univ. for Humanity, Russia
Yury Karpov	St. Petersburg State Technical Univ., Russia
Igor Kotenko	St. Petersburg Inst. for Informatics and Automation, Russia
Martin Kutter	AlpVision, Les Paccots, Switzerland
Anatoly Maliuk	Moscow State Engineering Physical Inst., Russia
Catherine Meadows	Naval Research Laboratory, USA
Nikolay Moldovian	Spec. Center of Program Systems "SPECTR", Russia
Vladimir Orlov	Microtest Company, Moscow, Russia
Gyorgy Papp	V.R.A.M. Communication Ltd., Hungary
Hartmut Pohl	Fachhochschule Bonn-Rhein-Sieg, St. Augustin-Univ. of Applied Sciences, Germany
Ravi Sandhu	SingleSignOn.Net Inc. and George Mason Univ., USA
Igor Sokolov	Inst. for Informatics Problems, Moscow, Russia
Mikhail Sycheov	Bauman State Technical Univ., Russia
Leonid Ukhlinov	The State Customs Committee of Russia, Russia
Vijay Varadharajan	Div. of Inf. and Commun. Sciences Macquarie Univ., Australia
Minerva M. Yeung	Media and Internet Technology, Intel, USA
Louise Yngstrom	Dept. of Comp. and Systems Sciences, Univ. & Royal Inst. of Technology, Stockholm
Peter Zegzhda	St. Petersburg State Technical Univ., Russia



## Reviewers

Kurt Bauknecht	Univ. of Zurich, Dept. of Information Technology, Switzerland
Kirill Bolshakov	St. Petersburg State Technical Univ., Russia
Dipankar Dasgupta	Div. of Comp. Science, Univ. of Memphis, USA
Gunther Drevin	Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Lynette Drevin	Comp. Science and Inf. Systems, Potchefstroom Univ., South Africa
Dimitris Gritzalis	Athens Univ. of Economics & Business, Greece
Vladimir Gorodetski	St. Petersburg Inst. for Informatics and Automation, Russia
Yury Karpov	St. Petersburg State Technical Univ., Russia
Igor Kotenko	St. Petersburg Inst. for Informatics and Automation, Russia
Evgenii Krouk	St. Petersburg State Technical Univ., Russia
Catherine Meadows	Naval Research Laboratory, USA
Nikolay Moldovian	Spec. Center of Program Systems “SPECTR”, Russia
Gyorgy Papp	V.R.A.M. Communication Ltd., Hungary
Vladimir Platonov	St. Petersburg State Technical Univ., Russia
Alexander Rostovtsev	St. Petersburg State Technical Univ., Russia
Ravi Sandhu	SingleSignOn.Net Inc. and George Mason University, USA
Michael Smirnow	GMD, FOKUS, Germany
Igor Sokolov	Inst. for Informatics Problems, Moscow, Russia
Vijay Varadharajan	Div. of Inf. and Commun. Sciences, Macquarie Univ., Australia
Dmitry Zegzhda	St. Petersburg State Technical Univ., Russia
Peter Zegzhda	St. Petersburg State Technical Univ., Russia

# Table of Contents

## Invited Talks

An Intelligent Decision Support System for Intrusion Detection and Response .....	1
<i>Dipankar Dasgupta, Fabio A. Gonzalez</i>	
Mathematical Models of the Covert Channels .....	15
<i>Alexander Grusho</i>	
Open Issues in Formal Methods for Cryptographic Protocol Analysis ....	21
<i>Catherine Meadows</i>	
Future Directions in Role-Based Access Control Models .....	22
<i>Ravi Sandhu</i>	
Secure Networked Computing .....	27
<i>Vijay Varadharajan</i>	
<b>Network Security Systems: Foundations, Models, and Architectures</b>	
Composability of Secrecy .....	28
<i>Jan Jürjens</i>	
Agent-Based Model of Computer Network Security System: A Case Study	39
<i>Vladimir I. Gorodetski, O. Karsayev, A. Khabalov, I. Kotenko, Leonard J. Popyack, Victor A. Skormin</i>	
Security Considerations and Models for Service Creation in Premium IP Networks .....	51
<i>Michael Smirnov</i>	
Secure Systems Design Technology .....	63
<i>Peter D. Zegzhda, Dmitry P. Zegzhda</i>	
A Privacy-Enhancing e-Business Model Based on Infomediaries .....	72
<i>Dimitris Gritzalis, Konstantinos Moulinos, Konstantinos Kostis</i>	
Applying <i>Practical</i> Formal Methods to the Specification and Analysis of Security Properties .....	84
<i>Constance Heitmeyer</i>	
Modeling Software Tools Complex for Evaluation of Information Systems Operation Quality (CEISOQ) .....	90
<i>Andrey Kostogryzov</i>	
Analyzing Separation of Duties in Petri Net Workflows .....	102
<i>Konstantin Knorr, Harald Weidner</i>	

**Intrusion Detection: Foundations and Models**

Information Security with Formal Immune Networks . . . . .	115
<i>Alexander O. Tarakanov</i>	
BASIS: A Biological Approach to System Information Security . . . . .	127
<i>Victor A. Skormin, Jose G. Delgado-Frias, Dennis L. McGee, Joseph V. Giordano, Leonard J. Popyack, Vladimir I. Gorodetski, Alexander O. Tarakanov</i>	
Learning Temporal Regularities of User Behavior for Anomaly Detection . . . . .	143
<i>Alexandr Seleznyov, Oleksiy Mazhelis, Seppo Puuronen</i>	
Investigating and Evaluating Behavioural Profiling and Intrusion Detection Using Data Mining . . . . .	153
<i>Harjit Singh, Steven Furnell, Benn Lines, Paul Dowland</i>	

**Access Control, Authentication, and Authorization**

Typed MSR: Syntax and Examples . . . . .	159
<i>Iliano Cervesato</i>	
TRBAC <sup>N</sup> : A Temporal Authorization Model . . . . .	178
<i>Steve Barker</i>	
The Set and Function Approach to Modeling Authorization in Distributed Systems . . . . .	189
<i>Tatyana Ryutov, Clifford Neuman</i>	
Fenix Secure Operating System: Principles, Models, and Architecture . . . . .	207
<i>Dmitry P. Zegzhda, Pavel G. Stepanov, Alexey D. Otavin</i>	

**Cryptography and Steganography: Mathematical Basis,  
Protocols, and Applied Methods**

Generalized Oblivious Transfer Protocols Based on Noisy Channels . . . . .	219
<i>Valeri Korjik, Kirill Morozov</i>	
Controlled Operations as a Cryptographic Primitive . . . . .	230
<i>Boris V. Izotov, Alexander A. Moldovyan, Nick A. Moldovyan</i>	
Key Distribution Protocol Based on Noisy Channel and Error Detecting Codes . . . . .	242
<i>Viktor Yakovlev, Valery Korjik, Alexander Sinuk</i>	
Dynamic Group Key Management Protocol . . . . .	251
<i>Ghassan Chaddoud, Isabelle Chrisment, André Schaff</i>	
SVD-Based Approach to Transparent Embedding Data into Digital Images . . . . .	263
<i>Vladimir I. Gorodetski, Leonard J. Popyack, Vladimir Samoilov, Victor A. Skormin</i>	
Fast Encryption Algorithm Spectr-H64 . . . . .	275
<i>Nick D. Goots, Alexander A. Moldovyan, Nick A. Moldovyan</i>	

CVS at Work: A Report on New Failures upon Some Cryptographic Protocols .....	287
<i>Antonio Durante, Riccardo Focardi, Roberto Gorrieri</i>	
On Some Cryptographic Properties of Rijndael .....	300
<i>Selçuk Kavut, Melek D. Yücel</i>	
<b>Author Index</b> .....	313